Groups and Group Actions

Richard Earl

Hilary and Trinity Terms 2013

Syllabus

Hilary Term (8 lectures)

- Axioms for a group and for an Abelian group. Examples including geometric symmetry groups, matrix groups (GL_n, SL_n, O_n, SO_n, U_n), cyclic groups. Products of groups. [2]

- Permutations of a finite set under composition. Cycles and cycle notation. Order. Transpositions; every permutation may be expressed as a product of transpositions. The parity of a permutation is well-defined via determinants. Conjugacy in permutation groups. [2]

- Subgroups; examples. Intersections. The subgroup generated by a subset of a group. A subgroup of a cyclic group is cyclic. Connection with hcf and lcm. Bezout's Lemma. [1.5]

- Recap on equivalence relations including congruence $\bmod n$ and conjugacy in a group. Proof that equivalence classes partition a set. Cosets and Lagrange's Theorem; examples. The order of an element. Fermat's Little Theorem. [2.5]

Trinity Term (8 lectures)

- Isomorphisms, examples. Groups up to isomorphism of order 8 (stated without proof). Homomorphisms of groups with motivating examples. Kernels. Images. Normal subgroups. Quotient groups; examples. First Isomorphism Theorem. Simple examples determining all homomorphisms between groups. [3]

- Group actions; examples. Definition of orbits and stabilizers. Transitivity. Orbits partition the set. Stabilizers are subgroups. [2]

- Orbit-stabilizer Theorem. Examples and applications including Cauchy's Theorem and to conjugacy classes. [1]

- Orbit-counting formula. Examples. [1]

- The representation $G \to \mathrm{Sym}(S)$ associated with an action of G on S. Cayley's Theorem. Symmetry groups of the tetrahedron and cube. [1]

Recommended Texts

- M. A. Armstrong Groups and Symmetry (Springer, 1997)

1. THE GROUP AXIOMS

1.1 Abstraction

Abstract algebra began as a twentieth century construct bringing together many nineteenth century results and observations. During the twentieth century, throughout much of pure mathematics, abstraction was to play an important role in shaping the subject. Prior to the nineteenth century, most mathematics had begun with some interest in real-world problems. Perhaps due to the paradigm-smashing discovery of non-euclidean geometries, nineteenth century mathematicians were more willing to cut that cord. In any case, thinking abstractly, mathematicians began looking at the underlying rules, logic and structures that drove seemingly disparate results. The power of abstraction, then, is its generality: beginning with the rules of an abstract structure, one can begin to demonstrate results that apply to all examples of that structure. Whilst the nature of a specific structure is likely grounded in some important concrete examples, the proof itself emerges independent of any particular examples. Still more, with luck, the proof will be that much more apparent as it focuses on the structure's rules only and there is no distraction from superficial clutter.

In this first course in abstract algebra we concentrate on *groups*. Two other important algebraic structures are *rings* and *fields* – you will likely have met the field axioms in Linear Algebra I and Analysis I. Both these concepts are due to Richard Dedekind (1831-1916) who was arguably the father of abstract algebra; certainly he was one of the first to fully appreciate the power of abstract structures. Fields and groups naturally lead to examples of groups also. Groups, particularly in the form of "substitution groups", had been apparent in the work of Galois, Gauss, Cauchy, Abel et al. in the early nineteenth century. The general axioms for a group were first written down by Cayley in 1849, but their importance wasn't acknowledged at the time; it wasn't until the 1870s that an appreciation of the merit of abstract structures was showing, especially in the nascent algebraic number theory which grew out of efforts to prove Fermat's Last Theorem.

1.2 Binary Operations

Definition 1 *A* ***binary operation*** $*$ *on a set* S *is a map* $* : S \times S \to S$. *We write* $a * b$ *for the image of* (a, b) *under* $*$.

So a binary operation takes two inputs a, b from S in a given order and returns a single output $a * b$ which importantly has to be in S. Standard examples include addition, multiplication and composition but there are many other examples as well.

Example 2 *The following are examples of binary operations.*

(i) $+, -, \times$ *on* $\mathbb{R}$*;* $\div$ *is not a binary operation on* $\mathbb{R}$ *as, for example* $1 \div 0$ *is undefined;*
(ii) $\wedge$*, the cross product, on* $\mathbb{R}^3$*;*
(iii) min *and* max *on* $\mathbb{N}$*;*
(iv) $\circ$*, composition, on the set* $\mathrm{Sym}(S)$ *of bijections of a set* S *to itself;*
(v) matrix multiplication on the set of $n \times n$ *complex invertible matrices (for a given* n*).*

Definition 3 *A binary operation* $*$ *on a set* S *is said to be* ***associative*** *if, for any* $a, b, c \in S$*,*

$$(a * b) * c = a * (b * c)\,.$$

In particular, this means an expression such as $a_1 * a_2 * \cdots * a_n$ *always yields the same result, irrespective of how the individual parts of the calculation are performed.*

Definition 4 *A binary operation* $*$ *on a set* S *is said to be* ***commutative*** *if, for any* $a, b \in S$*,*

$$a * b = b * a.$$

Definition 5 *An element* $e \in S$ *is said to be an* ***identity element*** *(or simply an* ***identity****) for an operation* $*$ *on* S *if, for any* $a \in S$*,*

$$e * a = a = a * e.$$

Proposition 6 *Let* $*$ *be a binary operation on a set* S *and let* $a \in S$*. If an identity* e *exists then it is unique.*

Proof. Suppose that e_1 and e_2 are two identities for $*$. Then

$$\begin{aligned} e_1 * e_2 &= e_1 && \text{as } e_2 \text{ is an identity;} \\ e_1 * e_2 &= e_2 && \text{as } e_1 \text{ is an identity.} \end{aligned}$$

Hence $e_1 = e_2$. ■

Definition 7 *If an operation* $*$ *on a set* S *has an identity* e *and* $a \in S$*, then we say that* $b \in S$ *is an* ***inverse*** *of* a *if*

$$a * b = e = b * a.$$

Proposition 8 *Let* $*$ *be an associative binary operation on a set* S *with an identity* e *and let* $a \in S$*. Then an inverse of* a*, if it exists, is unique.*

Proof. Suppose that b_1 and b_2 are inverses of a. Then

$$\begin{aligned} b_1 * (a * b_2) &= b_1 * e = b_1; \\ (b_1 * a) * b_2 &= e * b_2 = b_2. \end{aligned}$$

By associativity $b_1 = b_2$. ■

Notation 9 *If* $*$ *is an associative binary operation on a set* S *with identity* e*, then the inverse of* a *(if it exists) is written* a^{-1}*.*

Example 10 *If we look at the binary operations in Example 2 then we note:*
(i) $+$ *on* $\mathbb{R}$ *is associative, commutative, has identity* 0 *and* $x^{-1} := -x$ *for any* x*;*
$-$ *on* $\mathbb{R}$ *is not associative or commutative and has no identity;*
$\times$ *on* $\mathbb{R}$ *is associative, commutative, has identity* 1 *and* $x^{-1} := 1/x$ *for any nonzero* x*.*
(ii) $\wedge$ *on* $\mathbb{R}^3$ *is not associative or commutative and has no identity;*
(iii) min *on* $\mathbb{N}$ *is both associative and commutative but has no identity;*
max *on* $\mathbb{N}$ *is both associative and commutative and has identity* 0 *(being the least element of* $\mathbb{N}$*) though no positive integer has an inverse;*
(iv) $\circ$ *is associative, but not commutative, with the identity map* $x \mapsto x$ *being the identity element and as permutations are bijections they each have inverses;*
(v) matrix multiplication on $n \times n$ *invertible complex matrices is associative, but not commutative, with identity element* I_n *and* $A^{-1} := A^{-1}$ *(unsurprisingly);*

Remark 11 *Given a binary operation* $*$ *on* S *and a subset* $T \subseteq S$*, then we have a restriction* $* : T \times T \to S$ *which need not generally be a binary operation on* T*. We will, quite naturally, be interested in those subsets* T *for which* $*$ *restricts to a binary operation* $* : T \times T \to T$ *on* T*. In this case,* T *is said to be* ***closed*** *under* $*$*.*

Example 12 *The non-empty subsets* S *of* $\mathbb{Z}$ *to which* $+$ *restricts to a binary operation are those of the form* $m\mathbb{Z} = \{mn : n \in \mathbb{Z}\}$ *for some* m*.*

1.3 The Group Axioms

Definition 13 *A* ***group*** $(G, *)$ *consists of a set* G *and a binary operation* $*$ *on* G

$$* : G \times G \to G, \qquad (a, b) \mapsto a * b$$

such that
(i) $*$ *is associative – that is* $a * (b * c) = (a * b) * c$ *for any* $a, b, c \in G$*;*
(ii) there is an identity e *which satisfies* $e * a = a = a * e$ *for all* $a \in G$*;*
(iii) for each $a \in G$ *there exists an inverse* a^{-1} *such that* $a * a^{-1} = e = a^{-1} * a$*.*

Remark 14 *If the operation* $*$ *is clear and unambiguous then we will often simply say "*G *is a group" as a shorthand for "*$(G, *)$ *is a group".*

Remark 15 *When verifying that* $(G, *)$ *is a group we have to check (i), (ii), (iii) above and* ***also*** *that* $*$ *is a binary operation – that is,* $a * b \in G$ *for all* $a, b, \in G$*; this is sometimes referred to as* ***closure.***

Notation 16 *It is common notation to suppress the binary operation* $*$ *when discussing groups generally and instead to write* ab *for* $a * b$*. We shall do this from now on.*

Notation 17 *Also, when* n *is an integer, we will write*

$$a^n = \begin{cases} \underbrace{aaa\cdots a}_{n\ times} & n>0; \\ e & n=0; \\ \underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{-n\ times} & n<0. \end{cases}$$

Basic rules of algebra following from the group axioms are:

Proposition 18 *Let* G *be a group,* $x, y, z \in G$ *and* $m, n \in \mathbb{Z}$*. Then*
(a) $(xy)^{-1} = y^{-1}x^{-1}$.
(b) $(x^n)^{-1} = x^{-n}$.
(c) $x^m x^n = x^{m+n}$.
(d) $(x^m)^n = x^{mn}$.
(e) (Cancelling on the left) If $xy = xz$ *then* $y = z$*.*
(f) (Cancelling on the right) If $xy = zy$ *then* $x = z$*.*

Proof. Left as exercises. ■

Definition 19 *We say that a group* G *is* ***abelian,*** *after the Norwegian mathematician Niels Abel (1802-1829), if the group operation is commutative – that is,*

$$g_1 g_2 = g_2 g_1 \quad \textit{for all } g_1, g_2 \in G.$$

Example 20 *The sets* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ *form abelian groups under* $+$ *with* $e = 0$ *and* $x^{-1} := -x$ *in each case.*

Example 21 *The sets* $\mathbb{Q}\backslash\{0\}$, $\mathbb{R}\backslash\{0\}$ $\mathbb{C}\backslash\{0\}$ *form abelian groups under* $\times$ *with* $e = 1$ *and* $x^{-1} := 1/x$ *in each case. These groups are respectively denoted as* $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$.

Remark 22 *More generally if* $(F, +, \times)$ *is a field then* $(F, +)$ *and* $(F\backslash\{0\}, \times)$ *are both abelian groups.*

Example 23 *The set of positive real numbers* $(0, \infty)$ *form an abelian group under* $\times$ *with* $e = 1$ *and* $x^{-1} := 1/x$.

Example 24 *Any vector space forms an abelian group under* $+$.

Example 25 *Show that the* $n \times n$ *invertible real matrices form a group under matrix mutliplication. This group is denoted* $GL(n, \mathbb{R})$ *and is called the* n***th general linear group****.*

Show that $GL(n, \mathbb{R})$ *is non-abelian when* $n > 1$.

Solution. Our operation, matrix multiplication, is a binary operation because if A and B are invertible $n \times n$ real matrices then AB is invertible with $(AB)^{-1} = B^{-1}A^{-1}$.

Matrix multiplication is associative.

The group has an identity I_n as $I_n A = A I_n = A$ for all A and I_n is invertible.

Every element $A \in GL(n,\mathbb{R})$ has an inverse A^{-1} (in the usual sense) which is invertible as $\left(A^{-1}\right)^{-1} = A$ and which satisfies $AA^{-1} = A^{-1}A = I_n$.

If $n \geqslant 2$ then we see that

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & I_{n-2} \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & I_{n-2} \end{pmatrix}$$

don't commute as $(AB)_{11} = 2 \neq 1 = (BA)_{11}$ and hence $GL\left(n,\mathbb{R}\right)$ is non-abelian. ■

There are other important matrix groups. Let n be a positive integer.

Example 26 *The real invertible $n \times n$ matrices with determinant 1 form a group $SL(n,\mathbb{R})$ (the **special linear group**) under matrix multiplication which is non-abelian for $n \geqslant 2$.*

Example 27 *The orthogonal $n \times n$ matrices form a group $O(n)$ under matrix multiplication which is non-abelian for $n \geqslant 2$. (Recall a real matrix A is orthogonal if $A^{-1} = A^T$.)*

Example 28 *The orthogonal $n \times n$ matrices with determinant 1 form a group $SO(n)$ under matrix multiplication which is non-abelian for $n \geqslant 3$.*

Definition 29 *A complex square matrix A is called **unitary** if $A^{-1} = \overline{A}^T$, that is the transpose of the conjugate of A.*

Example 30 *Show that the unitary $n \times n$ matrices form a group $U(n)$ under matrix multiplication which is non-abelian for $n \geqslant 2$.*

Solution. This is left to Exercise Sheet 1, Question 3. ■

Example 31 *The set $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ forms an abelian group under multiplication. Note that the three groups S^1, $U(1)$, $SO(2)$ can all be naturally identified.*

An important (if rather elementary) family of groups is the *cyclic groups.*

Definition 32 *A group G is called **cyclic** if there exists $g \in G$ such that*

$$G = \left\{g^k : k \in \mathbb{Z}\right\}.$$

*Such a g is called a **generator**. As $g^i g^j = g^{i+j} = g^j g^i$ then cyclic groups are abelian.*

Example 33 *$\mathbb{Z}$ is cyclic and has generators 1 and -1.*

Example 34 *Let $n \geqslant 1$. The n**th cyclic group** C_n is the group with elements*

$$\left\{e, g, g^2, \ldots, g^{n-1}\right\}$$

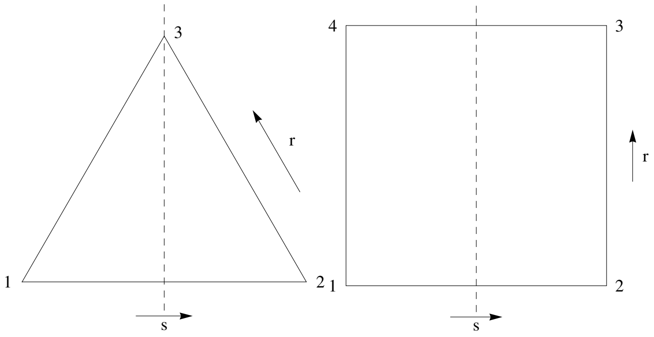
which satisfy $g^n = e$. So given two elements in C_n we define

$$g^i * g^j = \begin{cases} g^{i+j} & \text{if } 0 \leqslant i+j < n, \\ g^{i+j-n} & \text{if } n \leqslant i+j \leqslant 2n-2. \end{cases}$$

Another important family of groups is the *dihedral groups.*

Example 35 *Let $n \geqslant 3$ be an integer and consider a regular n-sided polygon P in the plane. We then write D_{2n} for the set of isometries of the plane which map the polygon back to itself. It is clear that D_{2n} forms a group under composition as (i) the identity map is in D_{2n}, (ii) the product of two isometries taking P to P is another such isometry, (iii) the inverse of such an isometry is another such isometry, (iv) composition is associative. Here "D" stands for "dihedral", meaning two-sided.*

We consider the $n = 3$ or D_6 case first, that is where the polygon is an equilateral triangle as in the first diagram below.



$n = 3$ $\qquad$ $n = 4$

We will denote rotation anticlockwise by $2\pi/3$ as r and denote reflection in the vertical as s. We will also label the vertices as $1, 2, 3$. It is easy to see that the following symmetries are all different

$$e, \qquad r, \qquad r^2, \qquad s, \qquad rs, \qquad r^2 s.$$

One way of seeing this is by noting how these symmetries permute the vertices; note that these six symmetries respectively permute the vertices as

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

In fact, these are the only symmetries of the triangle as there are $6 = 3!$ permutations of the vertices.

When $n = 4$ (i.e. when the group is D_8) we will similarly denote rotation anticlockwise by $\pi/2$ as r and again denote reflection in the vertical as s. If we will label the vertices as $1, 2, 3, 4$ then we note that the following eight symmetries are distinct because of their effect on the vertices:

$$\begin{aligned} e &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad r^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad r^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \\ s &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad rs = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \quad r^2 s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad r^3 s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}. \end{aligned}$$

What is slightly unclear in this case is whether there are any further symmetries. Clearly some permutations of the vertices cannot be performed as symmetries – for example, swappimg just 3 and 4 is not possible as, afterwards, 1 and 3 would no longer be opposite one another on a diagonal. We shall see in Proposition 36 that the eight symmetries above are indeed the only possible symmetries of the square.

Proposition 36 *Let P be a regular n-sided polygon P in the plane with r denoting anticlockwise rotation through $2\pi/n$ about P's centre and s denoting reflection in an axis of P. Then the symmetries of P are*

$$e, r, r^2, \ldots r^{n-1}, s, rs, r^2 s, \ldots r^{n-1} s. \tag{1.1}$$

Proof. Label the vertices of P as $1, 2, \ldots n$ in an anticlockwise order. Let t be a symmetry of P. Once t has been effected then the vertices will either read $1, 2, \ldots n$ anticlockwise or clockwise. Suppose the former and say that 1 has moved to position k where $1 \leqslant k \leqslant n$. Then $r^{1-k}t$ returns 1 to position 1 and – more generally, as the vertices are in an anticlockwise order – all vertices to their original starting positions. Hence $r^{1-k}t = e$ and we see $t = r^{k-1}$. If instead t changes the vertices to a clockwise order then ts – as s flips the polygon – keeps them in an anticlockwise order. As before we see that $ts = r^{k-1}$ for some $1 \leqslant k \leqslant n$ and hence $t = r^{k-1}s$ as $s^{-1} = s$.

Hence the symmetries in (1.1) are the only possible. To see that these $2n$ symmetries are distinct, well firstly each of $e, r, r^2, \ldots r^{n-1}$ keep the vertices in the same anticlockwise order but each moves vertex 1 to a different place, and each of $s, rs, r^2 s, \ldots r^{n-1} s$ reverses the order of the vertices and each moves vertex 1 to a different position. ■

Given two groups G and H, there is a natural way to make their Cartesian product $G \times H$ into a group. Recall that as a set

$$G \times H = \{(g, h) : g \in G, h \in H\}.$$

We then define the *product group* $G \times H$ as follows.

Theorem 37 *Let $(G, *_G)$ and $(H, *_H)$ be groups. Then the operation $*$ defined on $G \times H$ by*

$$(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$$

is a group operation. $(G \times H, *)$ is called the ***product group*** *or the* ***product of*** *G and H.*

Proof. As $*_G$ and $*_H$ are both associative binary operations then it follows easily from the definition to see that $*$ is also an associative binary operation on $G \times H$. We also note

$$e_{G \times H} = (e_G, e_H) \quad \text{and} \quad (g, h)^{-1} = (g^{-1}, h^{-1})$$

as for any $g \in G, h \in H$

$$\begin{aligned} (e_G, e_H) * (g, h) &= (g, h) = (g, h) * (e_G, e_H); \\ (g^{-1}, h^{-1}) * (g, h) &= (e_G, e_H) = (g, h) * (g^{-1}, h^{-1}). \end{aligned}$$

■

Definition 38 *The cardinality $|G|$ of a group G is called the* ***order*** *of G. We say that a group G is* ***finite*** *if $|G|$ is finite.*

One way to represent a finite group is by means of the *group table* or *Cayley table* (after the English mathematician Arthur Cayley, 1821-1895).

Definition 39 *Let $G = \{e, g_2, g_3, \ldots, g_n\}$ be a finite group. The* ***Cayley table*** *(or* ***group table****) of G is a square grid which contains all the possible products of two elements from G. The product $g_i g_j$ appears in the ith row and jth column of the Cayley table*

Remark 40 *Note that a group is abelian if and only if its Cayley table is symmetric about the main (top-left to bottom-right) diagonal.*

Example 41 *The Cayley table of D_6 is given below*

$*$	e	r	r^2	s	rs	r^2s
e	e	r	r^2	s	rs	r^2s
r	r	r^2	e	rs	r^2s	s
r^2	r^2	e	r	r^2s	s	rs
s	s	r^2s	rs	e	r^2	r
rs	rs	s	r^2s	r	e	r^2
r^2s	r^2s	rs	s	r^2	r	e

All these product can be worked out from just the three rules

$$r^3 = e, \qquad s^2 = e, \qquad sr = r^2 s.$$

So, for example, we see

$$\left(r^2 s\right)(rs) = r^2 (sr)\, s = r^2 \left(r^2 s\right) s = r^4 s^2 = r.$$

Proposition 42 *A Cayley group table is a latin square. That is, every group element appears precisely once in each row and in each column.*

Proof. Given a particular group element g_k we see that the map $G \to G$ given by $g \mapsto g_k g$ is a bijection with inverse $g \mapsto g_k^{-1} g$. This means that the kth row contains each element of G precisely once. Likewise the map $G \to G$ given by $g \mapsto g g_k$ is a bijection with inverse $g \mapsto g g_k^{-1}$, and this means that the kth column contains each element of G precisely once. ■

Example 43 *Note that, in both D_6 and D_8, the rotations by themselves – so $\{e, r, r^2\}$ when $n = 3$ and $\{e, r, r^2, r^3\}$ when $n = 4$ – make groups in their own rights. Their group tables are given below.*

$*$	e	r	r^2
e	e	r	r^2
r	r	r^2	e
r^2	r^r	e	r

,

$*$	e	r	r^2	r^3
e	e	r	r^2	r^3
r	r	r^2	r^3	e
r^2	r^2	r^3	e	r
r^3	r^3	e	r	r^2

We can see that these groups are the cyclic groups C_3 and C_4.

Put another way this means that $\{e, r, r^2\}$ is a subgroup of D_6 and $\{e, r, r^2, r^3\}$ is a subgroup of D_8.

Definition 44 *Let G be a group. We say that a subset $H \subseteq G$ is a* ***subgroup*** *of G if the group operation $*$ restricts to make a group of H. That is H is a subgroup of G if:*

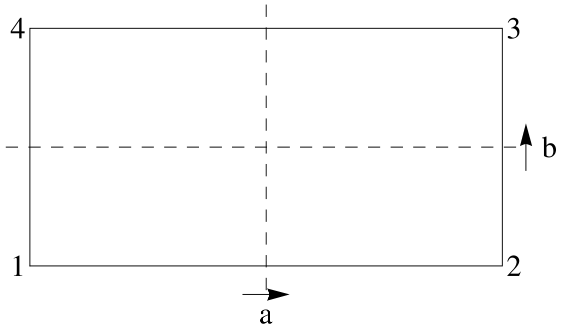
(i) $e \in H$;

(ii) whenever $g_1, g_2 \in H$ then $g_1 g_2 \in H$.

(iii) whenever $g \in H$ then $g^{-1} \in H$.

Note that there is no need to require that associativity holds for products of elements in H as this follows from the associativity of products in G.

Example 45 *If we consider the symmetry group of a (non-square) rectangle, then two symmetries are reflection in the vertical, which we will denote a, and reflection in the horizontal, which we will denote b. A further symmetry is ab which is rotation by π; we will write $c = ab$.*



If we label the vertices of the rectangle as $1, 2, 3, 4$ then we identify e, a, b, c as

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

These are in fact the only symmetries of the rectangle. To see this we only have to consider the position of vertex 1 after a symmetry has been effected; once we know where 1 has moved to then the positions of the remaining vertices are uniquely determined by the rectangle's geometry. The Cayley table for this group is then

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Note that the group is abelian.

This group – whether thought of in terms of the symmetries of a rectangle or considered as permutations – is often called the ***Klein four-group,*** *after the German mathematician Felix Klein (1849-1925) and denoted V or V_4. (The V stands for "vier", the German for "four".)*

Example 46 ***Groups of order four or less.*** *What ways are there to fill a Cayley table for a group of order $n \leqslant 4$? We will always have an identity element e and we will label the remaining element $a, b, c, \ldots$ depending on the order of the group.*

In the case $n = 1$, there is clearly only such table.

When $n = 2$ then the products e^2, ea, ae are all clear from the group axioms; further for the table to be a latin square we also need that $a^2 = e$.

When $n = 3$ then the products e^2, ea, ae, be, eb are all clear from the group axioms. Further we see that ab can be neither a nor b if the table is to form a latin square. The only remaining possibility is that $ab = e$ and likewise that $ba = e$. From there, the remainder of the table is uniquely determined on the basis of it being a latin square.

$\ast$	e
e	e

,

$\ast$	e	a
e	e	a
a	a	e

,

$\ast$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

.

The $n = 4$ situation is slightly more complicated. If we consider ba then it can (potentially) be either e or c.

Case (i): if $ba = e$ then $b = a^{-1}$ and so $ab = e$ also. (See first table below). But then, focusing on the third row and column, we must also have $bc = a = cb$ and $b^2 = c$. (See the second table below.) Finally, looking at the second row, we see that $a^2 = c$ and $ca = b = ac$ and $c^2 = e$ is the only remaining possibility. See final table.

$\ast$	e	a	b	c
e	e	a	b	c
a	a	?	e	?
b	b	e	?	?
c	c	?	?	?

,

$\ast$	e	a	b	c
e	e	a	b	c
a	a	?	e	?
b	b	e	c	a
c	c	?	a	?

,

$\ast$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

But is this a genuine group table? Note, in this case, that $c = a^2$ and $b = a^3$. If we swap the b and c rows and columns, we rewrite this table as

$\ast$	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

which we have already seen as a concrete example of a group, namely the four rotations of a square.

Case (ii) Instead now we consider the case $ba = c$. Likewise we can argue that $ab = c$.(See table below.) At this point, though, the way forward is still not clear, in the sense that we can continue to create a latin square in different ways. We could (potentially) have $a^2 = b$ or $a^2 = e$.

$\ast$	e	a	b	c
e	e	a	b	c
a	a	?	c	?
b	b	c	?	?
c	c	?	?	?

.

Case (ii)(a) Assuming $ba = c$ and $a^2 = b$ then we can complete the table (See first table below). But if we note $b = a^2$ and $c = a^3$ then we see we in fact have reproduced the same table as in case (i).

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

,

$*$	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

Cases (ii)(b') and (ii)(b") If we assume $ba = c$ and $a^2 = e$ then we can only complete the table as far as the first table below. We could still have either (b') $b^2 = a$ (see second table) or (b") $b^2 = e$ (see third table).

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	?	?
c	c	b	?	?

,

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

,

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

.

The second table again is nothing new as $a = b^2$, $c = b^3$, so that this is in fact the same group as we have just met twice already. But the final table is fundamentally different, for example as every element is self-inverse. We recognise it as the symmetry group of the rectangle or the Klein group V_4 that we met previously.

Remark 47 *In all, then, there are four latin squares of size 4×4 with first rows and columns (e, a, b, c). In each case, the latin square represented a group though this is not always the case (see Exercise Sheet 1, Question 2).*

To make the following discussion a little easier we introduce now the idea of the *order* of a group element.

Definition 48 *Let G be a group and $g \in G$. The* **order** *of g, written $\mathrm{o}(g)$, is the least positive integer r such that $g^r = e$. If no such integer exists then we say that g has infinite order.*

Remark 49 *Note, now, that there are unfortunately two different uses of the word order: the order of a group is the number of elements it contains; the order of a group element is the least positive power of that element which is the identity.*

In the above we have seen that *in essence* there is one group of order one, one of order two, one of order three and two of order four. Though the symbols for the elements may vary, an order two group consists of an identity element and an element of order two – so that it is in essence C_2; an order three group consists of an identity, an element of order three and its square – so that it is in essence C_3; an order four group either consists of an identity, an element of order four, its square and cube – so that is in essence C_4 – or it consists of an identity and three distinct elements of order two which commute – so that it is essentially V_4.

The idea which rigorously captures the idea of "in essence" is that of the *isomorphism.* For two groups to be the same "in essence" means that, suitably relabelled, their Cayley tables would be the same. That relabelling would be an isomorphism.

Definition 50 *An* ***isomorphism*** $\phi : G \to H$ *between two groups* $(G, *_G)$ *and* $(H, *_H)$ *is a bijection such that for any* $g_1, g_2 \in G$ *we have*

$$\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2).$$

Two groups are said to be ***isomorphic*** *if there is an isomorphism between them. Being isomorphic is fairly easily seen to be an equivalence relation. There may well be more than one isomorphism between isomorphic groups.*

The Cayley tables of two isomorphic groups would in essence be the same as follows. If $\phi : G \to H$ is an isomorphism and $G = \{g_1, \ldots g_n\}$ so that $H = \{\phi(g_1), \ldots, \phi(g_n)\}$ then ϕ would set up the following correspondence between the Cayley tables of G and H

$*_G$	g_1	$\cdots$	g_j	$\cdots$	g_n
g_1					
$\vdots$					
g_i			$g_i *_G g_j$		
$\vdots$					
g_n					

$\xrightarrow{\phi}$

$*_H$	$\phi(g_1)$	$\cdots$	$\phi(g_j)$	$\cdots$	$\phi(g_n)$
$\phi(g_1)$					
$\vdots$					
$\phi(g_i)$			$\phi(g_i) *_H \phi(g_j)$		
$\vdots$					
$\phi(g_n)$					

so that if the two tables are to properly correspond under ϕ we need to have in each case

$$\phi(g_i *_G g_j) = \phi(g_i) *_H \phi(g_j).$$

Remark 51 *We have seen that there are, up to isomorphism,* $1, 1, 1, 2$ *groups of order* $1, 2, 3, 4$ *respectively. In general it is a very difficult problem to work out how many groups there are of a given order. The number of different groups* g *for each order* n *up to* 80 *are given in the table below.*

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
g	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1	5	1	5
n	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
g	2	2	1	15	2	2	5	4	1	4	1	51	1	2	1	14	1	2	2	14
n	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
g	1	6	1	4	2	2	1	52	2	5	1	5	1	15	2	13	2	2	1	13
n	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
g	1	2	4	267	1	4	1	5	1	4	1	50	1	2	3	4	1	6	1	52